Claim to be an internal caller having difficulty dialing out and ask for an outside line.

Auto Attendant

"Dupe the system and your switchboard operator"

Access your Automated Attendant via 1-800 trunks and dial an invalid # or allow to default to the PBX Attendant.

Fraudulent caller does not speak, and the attendant assumes a dead call and releases.

Before the connection breaks down, caller dials "9" and gets an outside line.

Auto Attendant and Voice Mail

"Thru-Dial"

Access via 1-800 trunks into Auto Attendant or Voice Mail.

When asked to enter desired extension number, 91XX or 9011 is entered.

Auto Attendant attempts a transfer to extension 91XX or 9011, which to the PBX is an outgoing toll call, and the caller dials the balance of the digits required.

The same process applies if the access was to any mail box and "thru-dial" out of voicemail is not fully restricted.

DISA (Direct Inward System Access)

If access is via 1-800 trunks, this is a likely target for Professionals.

Finding a DISA 800 number is the dream of every hacker.

Hacker or Professional finds the Disa trunk by dialing 800 numbers and listening for a DISA tone prompt.

Simple matter to break the PIN or Authorization Code especially if;

Short Codes.

Predictable Codes.

Unchecked Codes.

Multiple Codes.

If there are no dialing restrictions on the codes, your facilities are now wide open.

AT&T Call Manager (ACM)

ACM is a service from AT&T that is an enhanced, value added account billing service generally known as Sub Account Billing (SAB).

Allows (0+) ACM call to be billed at (1+) direct dial rates and provides billing sorted by user account code provided by the caller.

No subscription is required.

How it works!

Caller dials (using AT&T long distance) 0+ or (1+0+288+0) plus the destination telephone number.

Caller receives AT&T bong tone and dials ACM code plus (XXXX).

The (XXX) is any four digits the caller wants to use as an account code for the billing on the call.

Subsequent calls can be made by dialing (#) after called party hangs up.

No screening or validation is provided on the account code.

ACM - So what's the problem?

A common toll restriction scheme is to deny 1+ calls but to allow 0+ calls for operator assisted or credit card calls. ACM allows the caller to bypass this restriction and place calls billed directly as a 1+ call.

DISA outgoing toll restriction is bypassed allowing calls to be placed through the system once the DISA code is broken which would otherwise have been somewhat limited.

Lobby and other restricted phones on premise are also now unrestricted.

What can be done?

Re-evaluate PBX feature usage and toll restriction plan.

Subscribe to Originating Line Screening (GTE calls it Selective Class of Call Screening) from the LEC on every trunk to provide Central Office screening on the trunk.

> The LEC passes ANI with a screening indicator to AT&T which if the ANI appears in a Negative SAB database the caller receives the following announcement:
>
> "The service you have requested is not available to you."

Attempt to get AT&T to provide ACM on a subscription basis only.

Who Pays ??? $$$$$$$$

YOU DO !!!!

No Long Distance Carrier covers the cost of a subscriber' fraud.

F.C.C. Tariff - Liability of the Carrier

> "The Carrier is not responsible for any damages, including toll usage

> charges, the subscriber may incur as a result of the unauthorized use of its telephone facilities. This unauthorized use of the subscriber's facilities includes, but is not limited to, the placement of calls from the subscriber's premises, and the placement of calls through subscriber-provided equipment which are transmitted or carried on the [carrier's] network. The [carrier's] Security Department may work with the subscriber to recommend possible solutions to reduce unauthorized use of their facilities. However, [the carrier] does not warrant or guarantee that its recommendations will prevent all unauthorized use, and the subscriber is responsible for controlling access to, and use of, its own telephone facilities."

F.C.C. rulings to date state that the cost of Fraud be paid by the business that uses the equipment rather than by the supplier of the equipment or services.

Only the owner / user of the PBX can stop access to their equipment.

Unlike Credit Cards, there is no limit to your liability!

WHAT ARE THE MANUFACTURERS DOING?

All major PBX and Voice Mail manufacturers are adding additional controls to inhibit hackers.

Note; You will be required to pay for these upgrades or they may only be available on their latest product line.

- Expanded and variable length passwords and authorization codes.
- Additional dialing classes of service and restrictions.
- Table restrictions for Access Codes and Area Codes.
- Forced password changes.
- Lockouts for invalid attempts.

WHAT ARE THE CARRIERS AND THE TELCOS DOING?

Education

"High Toll" Gates (Future)

WHAT CAN YOU DO?

DETECTION

Monitor Usage - Call Accounting System

Look for multiple short duration calls which may indicate hacking attempts, especially after hours. (Ensure your system is recording short duration calls.)

If you have ANI (Automatic Number Identification available on Primary Rate ISDN), check the area code origin of all 800 In-Wats calls. Look for calls from area codes 212 or 218 (New York).

Look for inappropriate time of day calls; ie, after hours and weekend calls.

Increase in activity and/or data storage levels of your call accounting equipment.

Significant increase in-Wats or Out-Wats and/or international calls.

Ensure that your call accounting system can track Trunk-to-Trunk calls.

Monitor user complaints

Complaints of difficulty in making or receiving external calls, which may indicate that your facilities are being tied up by fraudulent calls.

Reports that false 911 calls have been placed from your business.

Switchboard operators may notice an increase in outside callers asking internal users what number or party they've reached.

Switchboard operators receiving a large number of dead air calls.

Reports of lots of wrong or obscene calls.

PREVENTION

DISA Fraud Prevention

Remove DISA feature and utilize credit cards. (More expensive, but you have a liability limit.)

Use the maximum number of digits available for PIN or Authorization Code and change them periodically.

Program a Disconnect upon invalid password attempt.

Program DISA port to not return Prompt Tone.

Program DISA port to answer only after 5 rings.

If you have individual PINs or Authorization Codes for individuals or departments, change them periodically and be sure to delete them for any terminated employee.

Program appropriate class of service call restrictions for every valid code.

Program Time of Day access to Disa. Limit your exposure!

Voice Mail Thru-Dial

Beware! This is the most recent avenue of access discovered by professionals. It has the highest potential dollar impact. Because it is a recent phenomenon, most Voice Mail Systems and PBXs may not have sufficient blocking coded into the software. It is your responsibility to ensure your system is secure and to monitor it to ensure it remains secure.

Have your Vendor review your current configuration and you should then attempt to "hack" your own system.

Although "thru-dial" is a viable feature for transferring out of Voice Mail to an internal extension, review very carefully any "out-dial" applications and consider removing if not necessary.

Most PBX Vendor proprietary Voice Mail systems have thru-dial restriction configurations available. Be more careful of outboard systems. Try dialing extension 9011 from a voice mailbox or automated attendant.

General Precautions

Remember, your systems will be hacked. New methods of access will be found. Holes or errors in the current configuration will be found. The Administration ports may be "hacked" and configuration changes could be made.

The following are good secondary restrictions which may limit the impact of any penetration which occurs:

Restrict by time-of-day access to long distance trunk routes.

Restrict international calls to countries that your business has no reason to call.

Require the use of Checked Forced Account Codes for all international calls. (Maximum Length and Random Numbers)

Program DISA trunks to;

- disconnect after invalid Forced Account Code
- not return DISA prompt tone
- answer after 5 rings

If international calling is absolutely required, consider setting aside one or two trunks with a unique (confidential) Access Code as well as a Forced Account Code. Remove this trunk group from the normal least cost routing scheme.

Configure the PBX to allow only preprogrammed international telephone numbers programmed into System Speed Tables.

Have your long distance carrier block incoming access to your 800 number from areas of the country where you do not do business. Block Area codes 212 and 218 (New York City) in particular. Provide Calling Card for this area if necessary.

Have your long distance carrier block out-going international calls at least to countries you do not do business with.

Establish dialing restrictions in each piece of equipment even if it is redundant; ie, if possible, program international restrictions on Voice Mail out-dial, PBX trunk routing, and carrier access.

Never leave any default passwords in any system.

Monitor your system performance and all reports and long distance bills.

Report any suspected abuse immediately to your long distance carrier and equipment vendors.

Destroy telephone-system information that might be useful to hackers. "Dumpster Diving"

Password protect all modems associated with your PBX or its outboard systems; ie, Voice Mail.

ANCILLARY PRODUCTS

Call Accounting Systems

- Allows you to detect Fraud.

- You must run reports daily and look for Fraud.

eg: Pacific Mutual was hit for $200,000 in only four days over a weekend. What would it have been if they were not monitoring their reports?!!

System Requirements

Must be able to track Trunk-to-Trunk calls in order to record DISA and Voice Mail thru-dial Fraud. (Most systems track only internal stations or account codes and may miss the fraudulent calls.

Your system must also be programmed to record short calls. This is often intentionally excluded from reports.

Should be easy to use and automatically print various reports that make it easy to identify;

- after hours calling patterns
- international calls
- ANI on ISDN primary rate circuits

Dial Back Modems

Features

Standard Call Back to pre-programmed telephone number by authorization code dialed.

Programmed Call Back for mobile users by authorization code.

Pass - Through by authorization code. (This at least requires the hacker to crack an additional password.)

Audit Trail Reports that lists all access attempts, authorization codes, time of day, and telephone number of Programmed Call Back.

Third Party Remote Access (DISA) Boxes

Provide multilevel passwords for different access privileges.

Dial Back capability by authorization code.

Can be used for many other devices; ie,

- Voice Mail and PBX Administration Ports
- Dictation equipment
- Paging
- Modems
- Remotely Controlled Systems (security, lighting, heating and air conditioning, etc.)

SUMMARY

Every PBX and Computerized System is potentially the target of "**Hackers**" and professional criminals.

No Manufacturer or Vendor of PBX systems can develop and install computerized systems that are totally invulnerable to unauthorized invasion, use, abuse, or damage.

The End User must select and implement that combination of features which best meets their needs, recognizing the trade-offs between security, convenience and flexibility.

Ultimately, it is the End User's responsibility to monitor their system in order to detect Hackers and Fraud, and to initiate those changes in their system that may block that particular type of access.

DISCLAIMER

This information is being provided as a service to our customers and is not intended as a warranty. GTE disclaims all liability arising in connection herewith. No express or implied warranty is made against the fraudulent use of the telephone systems.

ATTACHMENT B

IT'S EASY TO USE YOUR GTE CALLING CARD.

These easy-to-follow instructions are printed on the back of your card for your convenience.

From Touch-Tone Phones

1. Press "0" plus the area code and the number you're calling. For local calls, do not enter the area code.
2. Wait for the tone, then enter your GTE Calling Card number.
3. To make consecutive calls, don't hang up; just press the "#" button and enter the next phone number.

From Rotary Phones

1. Dial "0" plus the area code and the number you're calling. For local calls, do not dial the area code.
2. When the operator answers, say, "Calling Card number. . . ," and state your calling card number.
3. To make consecutive calls, briefly press the switch-hook, and the operator will place your next call.

From GTE Card-Reader Phones

Simply follow the directions provided on the GTE telephone you're using. To make consecutive calls, don't hang up; just press the "#" button and enter the next phone number.

PROTECT YOUR PIN

Your 4-digit Personal Identification Number (PIN) is confidential, and can help you guard against calling card fraud. To protect yourself and your calling card, GTE suggests you use these precautions:

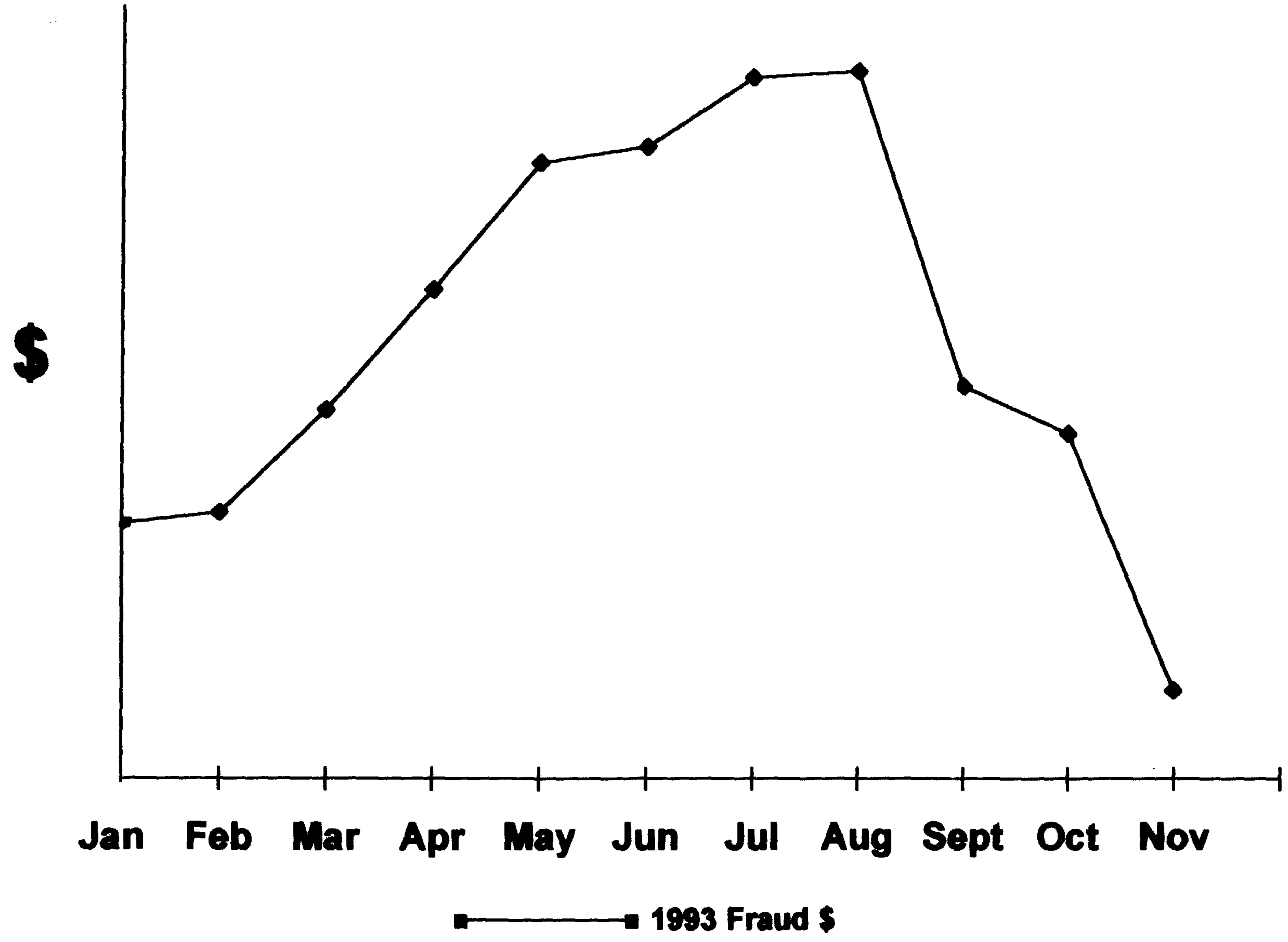
1. Memorize your card number, so you don't need to take out your card in a public place. Your GTE Calling Card number is easy to remember, because it's your telephone number plus your 4-digit PIN.
2. Don't give out your card number to others. If someone contacts you claiming to work for the telephone company and requests your calling card number, do not divulge this information. Instead, contact your local telephone company business office. If you have given your card number to anyone, please call the business office and have a new PIN assigned. International travelers should contact their long-distance company for instructions concerning calls made from foreign countries to the U.S.
3. Be wary of loiterers who may be watching as you dial.
4. If you do take out your card in a public place, block it from view and try to block the dial, too.
5. Report all lost, stolen or misplaced cards immediately by calling the number of your local GTE business office, which can by found in your GTE Directory.
6. The card should never be used after the telephone service or account to which the charges incurred are billed has been discontinued. If your telephone number is changed or service is discontinued, please destroy your old card to protect yourself against unauthorized charges by others.

If you move from your present address and your telephone number changes, please request a new GTE Calling Card.

Licensed under U.S. Patent B1 4,034,210

ATTACHMENT C

Calling Card Fraud


$
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sept
Oct
Nov
1993 Fraud $